



Data Retention Policy

Version 1 - Approved by Rishabh



Contents

1. [Objective](#)
2. [Scope](#)
3. [Policy Statement](#)
4. [Data Retention Guidelines](#)
5. [Document Security Classification](#)
6. [Non-Compliance](#)
7. [Responsibilities](#)
8. [Schedule](#)
9. [Version History](#)



1. Objective

Customers and users of Superhawk AI may request the deletion of data that belongs to them from our systems. This policy outlines the provisions we provide for such requests and describes how such requests should be handled.

2. Scope

This policy applies to all customer and user data collected, processed, or stored by Superhawk AI across our SaaS platform, including Personal Identifiable Information (PII), business and operational data, and behavioral data. Covered storage locations include cloud platforms we utilize (AWS and GCP) and corporate employee devices (laptops/workstations) when such devices store customer data. The scope includes data received from customers or users and data generated through use of Superhawk AI products or services, including data produced during testing, alpha/beta, or early access programs.

3. Policy Statement

Data retention is based on valid reasons, and customers can request the deletion of their information. Requests should be authenticated and evaluated for legitimacy. Deletion may be withheld if it disrupts services. Anonymization of personal data may be considered before deletion, except where prohibited.

4. Data Retention and Deletion Guidelines

- All customer and user data is retained only while there is a lawful, contractual, or business need to do so. Retention periods are defined per data category and contractual agreement with the customer, taking into account applicable laws (e.g., GDPR).
- Customers and users may request deletion by submitting a written request via the customer portal or to support@. Requests must include sufficient identification details to validate the requestor's identity; for account holders this may include account email and order identifiers. Support and identity verification steps are documented in the Data Subject Request procedure.
- Data Retention Guidelines: - Superhawk AI classifies data by sensitivity (e.g., PII, business data, behavioral data) and applies retention periods documented in our retention schedule. The retention schedule references legal, regulatory, and contractual requirements and is reviewed annually. - Deletion requests are evaluated for authenticity and legitimacy by Support in coordination with Legal and the Information Security function. Deletion requests from customers with active contracts will be assessed against contractual obligations and potential service disruption; where deletion would disrupt active service, alternatives such as data export or scoped deletion will be discussed.
- Data Deletion Guidelines: - Deletion is initiated upon customer request, contract termination, or at the end of the retention period specified in the customer agreement, subject to verification and legal holds. Deletion is not performed where retention is required to meet legal obligations, resolve disputes, enforce agreements, or for other legitimate purposes documented by Legal. - For data



stored in cloud services (AWS and GCP), Superhawk AI relies on vendor-managed controls for secure deletion and lifecycle management of stored objects and volumes. Where applicable, logical deletion is performed in application databases and object storage followed by physical removal according to cloud provider APIs and our retention schedules. Backups managed by Superhawk AI's cloud configurations are retained and purged according to our backup retention policy; recovery from backups may prevent immediate permanent removal until backup retention cycles expire. - For data residing on employee devices, data subject to deletion will be removed from corporate-managed devices via endpoint management processes; if personal devices outside corporate control contain customer data, deletion actions are coordinated with the device owner and documented. - When feasible and appropriate, anonymization/pseudonymization is considered as an alternative to deletion where it satisfies the request and complies with laws and contracts. - A record of all deletion requests and the actions taken, including timestamps, the scope of data removed, and responsible personnel, will be maintained in our ticketing system for accountability and compliance verification. - Company policy documentation versions and older policy versions will be retained for at least six years.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer and the Data Protection Officer (DPO) where applicable are responsible for approving and reviewing this policy and related procedures. The Support team is responsible for receiving and initiating deletion requests; Legal must be consulted for requests involving legal holds, active disputes, or contractual retention requirements. Engineering is responsible for executing deletions in application databases, object storage (AWS/GCP), and coordinating with cloud administrators. IT/Endpoint Management is responsible for removing data from corporate devices. All staff and contractors must follow this policy and report data deletion requests to Support.

8. Schedule

This document shall be reviewed annually and additionally reviewed whenever there are significant changes to our cloud providers (AWS or GCP), data processing activities, applicable laws (e.g., GDPR), major changes to product architecture, or incidents that materially affect data deletion practices.



End of Data Retention Policy. For version history, please see the next page.



Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026